REMARKS

In the Office Action under reply, claims 3, 8, 13, 23 and 26-29, all the claims remaining in this application, were rejected under 35 USC 103 once again as being unpatentable over the combination of Rosner (U.S. Patent 6,636,968), Kato (6,381,331) and Schneier ("Applied Cryptography"). Claims 3, 8, 13, 18 and 23 are the only independent claims. Claims 26-29, depend from claims 3, 8, 18 and 23.

On considering the Examiner's stated rejections and his response to the arguments presented in the Amendment filed September 20, 2007, it is believed some of Applicants' claim recitations are being interpreted in a manner inconsistent with Applicants' specification. To obviate such an unwarranted interpretation, the independent claims are amended to clarify that which had been expressed previously.

It is respectfully submitted that the claims present in this application are patentably distinct over the combination of Rosner, Kato and Schneier for the reasons now discussed.

All the claims present in this application recite the feature that is best found in claim 3 as follows:

> generating on the basis of said encryption key, sets of passkeys, each set having at least two passkeys and each set of passkeys specific to a respective one of said specific destinations by dividing said encryption key by a division pattern that is: (a) unique to each of said specific destinations and (b) based on the content of said digital data;
>
> generating a plurality of partial keys based on a portion of the passkeys in said set or a portion of passkey information from which said passkeys may be reproduced;
>
> delivering either said plurality of partial keys or partial key information, from which said partial keys may be reproduced, and delivering the remaining passkeys in a set not used to generate said partial keys or the remaining passkey information, to a respective one of said specific destinations over a plurality of delivery routes which differ from routes for delivering said digital data and which are further different from each other ...

See, for example, paragraphs [0025]-[0027], [0093], [0095] and [0118] of Applicants' corresponding published application.

It is respectfully submitted, the combination of references relied upon in the Office Action under reply fails to suggest the limitations quoted above. Rosner, describes a "session key" K that is based upon a secret key x from the source, or upstream encrypting device, and public keys Y1, Y2, Y3 and Y4 from destination devices. Rosner also mentions that partial keys X1, X2, X3 and X4 are generated by the key generator 220; and these partial keys are created such that "a knowledge of the private key ... of each corresponding destination device ... and a knowledge of a common group key ... facilitates a determination of a decryption key ... that is suitable for decrypting the encrypted content material." There is no description in Rosner of dividing session (or encryption) key K by a unique pattern to produce the partial keys. Indeed, there is no description of how Rosner's partial keys X1, X2, X3 and X4 are created. Equation (1) of Rosner sets forth the mathematical representation of the partial key Xj (where j is 1, 2, 3,...), where Xj is a function of the public key Y from a destination device. It is clear from Rosner's equation (1) that his partial keys X are not produced by dividing his encryption K by any pattern.

Assuming arguendo that Rosner's partial keys X1, X2, X3 and X4 are interpreted as corresponding to Applicants' claimed passkeys, Rosner's keys X1, X2, ... would have to be generated "by dividing said encryption key [assumed to be Rosner's key K] by a division pattern." Rosner fails to suggest that his keys X1, X2, ... are generated by dividing his key K by anything, much less a division pattern. In addition, for Rosner's keys X1, X2, ... to correspond to Applicants' claimed passkeys, the division pattern used to divide key K must be unique to the specific destination to which those partial keys are sent. Moreover, each of Rosner's destinations

must be supplied with a set of passkeys (a set has at least two passkeys); but Rosner describes only one key X1 (or X2, ...) that is sent to a destination. This is far from being a "set" of passkeys. And, finally, for Rosner's keys X1, X2, ... to correspond to Applicants' claimed passkeys, those keys X1, X2, ... must be based on the content being encrypted. Rosner fails to link his keys X1, X2, ... to his content material being encrypted -- and the Examiner correctly recognizes this deficiency of Rosner.

In discussing Rosner at page 4, lines 16-21 of the Office Action under reply (the Examiner is thanked for providing the convenience of numbering the lines in his Office Action), the Examiner correctly observes that Rosner's keys X1, X2, ... are specific to each destination. However, these keys X1, X2, ... are not "generat[ed] on the basis of said encryption key (K);" nor are they generated by dividing the encryption key K by a division pattern. As discussed above and as is seen from Rosner's equation (1), there is no link between encryption key K and keys X1, X2, ... Nor does Rosner suggest that keys X1, X2, ... should be generated by dividing encryption key K. The factors X^{y1}, X^{y2}, ... mentioned in the Office Action are sub keys created at each destination device (see Rosner, col. 5, lines 14-33) for the purpose of decryption. Rosner does not suggest that these factors should or could be used at the encrypting device to divide encryption key K so as to produce a set of keys X1, X2, ... Fig. 4 of Rosner illustrates, in blocks 250, 260, etc. that $X1=K1/X^{y1}$, $X2=K2/X^{y2}$, etc. But Fig. 4 and its associated text represent the decryption sub key at each destination device. Fig. 4 does not suggest that key X1 should be generated by dividing encryption key K by anything.

The foregoing discussion of Rosner is based upon the assumption that his keys X1, X2, ... correspond to Applicants' claimed passkeys. It is possible that an effort may be made to interpret Rosner's keys X1, X2, ... as corresponding to Applicants' claimed "partial keys." But

Applicants' partial keys are "based on a portion of the passkeys." Hence, if Rosner's keys X1, X2, ... correspond to Applicants' partial keys, there is nothing left in Rosner that corresponds to Applicants' passkeys.

Notwithstanding the failure of Rosner to describe dividing his encryption key K by a division pattern, the Examiner correctly notes that Rosner fails to describe a division pattern "based on the content of said digital data." However, the Examiner turns to Kato for an alleged teaching that "the encryption keys used to encrypt the content should be prepared for each content (See Kato Col. 10 Lines 37-52)." It is respectfully submitted that Kato fails to encrypt with an encryption key based on the content being encrypted. Kato uses different encryption keys for different blocks of content. See col. 6, lines 61-64 of Kato. Key K1 encrypts one block and K2 encrypts another block. This is what Kato means by "[t]he keys K1, K2 and Tk are prepared in units of contents" (col. 10, line 46, emphasis added). But, these blocks and Kato's keys K1 and K2 have nothing to do with the content of a block.

The Examiner also notes, correctly, that Rosner fails to describe generating a plurality of partial keys based on a portion of the passkeys in a set. But, the Examiner contends that Schneier "teaches that keys should be split using random numbers" and this meets Applicants' claimed recitation of "generating a plurality of partial keys based on a portion of the passkeys in said set." Applicants respectfully disagree with this interpretation of Schneier. As argued in the amendment filed September 20, 2007, Schneier is silent with respect to generating partial keys based on a portion of the passkeys which, in turn, are generated by dividing the encryption key. While paragraph 1 at page 177 of Schneier speaks to distributing keys by splitting a key into several parts, there is no disclosure (at least in the portion of Schneier furnished to Applicants'

representative) of generating the key that is thus split into parts from an encryption key by dividing that encryption key by a unique division pattern.

As also argued in the amendment filed September 20, 2007, Schneier fails to suggest that a key should be split by dividing it by a division pattern, as recited in Applicants' claims. However, the Examiner contends that Schneier "teaches that the key should be split using random numbers, which would be unique for each splitting (See Schneier Pages 70-71 Section 3.6 Secret Splitting)." But here, Schneier describes an alternative to enciphering by using a key, that is, an alternative to key enciphering. Schneier's Secret Splitting discussion sends a message that is encrypted using an exclusive-OR (XOR) operation that XORs the message with, for example, three random-bit strings to generate an enciphered message. The original message can be deciphered by XORing the enciphered message with all three of the random-bit strings. Clearly, there is no teaching of splitting an encryption key because Schneier describes this XOR technique as an alternative to key encryption. Furthermore, there is no splitting of a message because the message simply is XORed with bit strings -- nothing is split or divided. In fact, the last sentence in Schneier's Secret Splitting section 3.6 states: "Remember, M [the message] isn't being split in the normal sense of the word; it is being XORed with random values."

It is improper to attempt to interpret Schneier in a manner that is inconsistent with Schneier's teachings: Schneier XORs a message with random values -- he does not divide an encryption key by a division pattern to generate a set of passkeys; nor does he generate partial keys based on a portion of those passkeys.

In commenting on Applicants' arguments presented in the amendment filed September 20, 2007, the Examiner refers to Applicants' admission at page 10, lines 12-14 of that amendment that Schneier teaches dividing a message. Applicants' representative apologizes for

incorrectly explaining Schneier's disclosure. Section 3.6 of Schneier describes XORing a message M with random values R, S and T. It was incorrect for Applicants' representative to characterize this XOR operation as "dividing a message into pieces."

Referring to lines 11-16 of the Examiner's response, at page 3 of the Office Action under reply, to Applicants' arguments regarding Schneier as set out in the amendment filed September 20, 2007, Applicants repeat:

- Contrary to the Examiner's interpretation of the reference, Schneier doe not disclose dividing keys.
- Contrary to the Examiner's interpretation of the reference, Schneier doe not disclose the use of a division pattern. It is improper to characterize Schneier's random-bit strings R, S and T as being "division patterns."

Therefore, for the reasons discussed above, neither Rosner, nor Kato nor Schneier, alone or in combination, describe or suggest Applicants' claimed recitations;

> generating on the basis of said encryption key, sets of passkeys, each set having at least two passkeys and each set of passkeys specific to a respective one of said specific destinations by dividing said encryption key by a division pattern that is: (a) unique to each of said specific destinations and (b) based on the content of said digital data;
>
> generating a plurality of partial keys based on a portion of the passkeys in said set or a portion of passkey information from which said passkeys may be reproduced;
>
> delivering either said plurality of partial keys or partial key information, from which said partial keys may be reproduced, and delivering the remaining passkeys in a set not used to generate said partial keys or the remaining passkey information, to a respective one of said specific destinations over a plurality of delivery routes which differ from routes for delivering said digital data and which are further different from each other ...

Therefore, even if an attempt is made to assemble the teachings of these references in an effort to reconstruct the prior art, the result still would not be suggestive of the aforequoted

features recited in all of Applicants' claims. Accordingly, claims 3, 8, 13, 18, 23 and 26-29 are in condition for allowance because these claims recite features not found in the prior art relied upon by the Examiner. An early notice to that effect is respectfully urged.

Please charge any additional fees that may be needed, and credit any overpayment to our Deposit Account No. 50-0320.

Respectfully submitted,

FROMMER LAWRENCE & HAUG LLP
Attorneys for Applicants

By: 
William S. Frommer
Reg. No. 25,506
(212) 588-0800